Article

A Mechanism of Masking Identification Information regarding Moving Objects Recorded on Visual Surveillance Systems by Differentially Implementing Access Permission

Namje Park ^{1,2} , Byung-Gyu Kim ^{3,*} and Jinsu Kim ²¹ Department of Computer Education, Teachers College, Jeju National University, Jeju City 63243, Korea² Cybersecurity Human Resource Institute, Jeju National University, Jeju City 63243, Korea³ Department of IT Engineering, Sookmyung Women's University, Seoul 04310, Korea

* Correspondence: bg.kim@sookmyung.ac.kr

Received: 13 May 2019; Accepted: 26 June 2019; Published: 28 June 2019

Abstract: Video surveillance systems (VSS), used as a measure of security strengthening as well as investigation, are provided principally in heavily crowded public places. They record images of moving objects and transmit them to the control center. Typically, the recorded images are stored after being encrypted, or masked using visual obfuscations on a concerned image(s) in the identification-enabling data contained in the visual information. The stored footage is recovered to its original state by authorized users. However, the recovery entails the restoration of all information in the visual data, possibly infiltrating the privacy of the object(s) other than the one(s) whose images are requested. In particular, Artificial Intelligence Healthcare that checks the health status of an object through images has the same problem and must protect the patient's identification information. This study proposes a masking mechanism wherein the infiltration of visual data privacy on videos is minimized by limiting the objects whose images are recovered with differential use of access permission granted to the requesting users.

Keywords: surveillance; masking identification; access permission; video surveillance; CCTV

1. Introduction

Video surveillance systems (VSS), which increase protection against physical infiltrations in public places or private buildings/facilities or monitor fire incidents inside buildings/facilities, are installed principally in heavily crowded areas to help prevent violent crimes or incidents/accidents such as cases of lost children or property and kidnapping. Video images recorded on VSS are stored real-time on storage devices. The recorded visual information is sent to a closed circuit television (CCTV) control center that supervises the VSS device concerned, and to administrator(s) there with proper access rights. The information is then made available for preventing possible incidents/accidents in target area(s), and for understanding the root cause of and investigating any incidents/accidents once they have occurred, and presenting evidence for resolving situations [1–4].

CCTV control centers are authorized to control the majority of the CCTV in target area(s) that are provided by respective local governing bodies. The centers also have access permission to video images that are recorded. Personal information, which can identify an individual whose images are included in the video recording, should be recoverable since it can be used for traceability later on. With this in mind, all identification information recorded, if any, is subject to full-scale masking, or the entirety of the visual data is encrypted to prevent leakage by a third party. However, when images are recovered by a legitimate user with access rights, all of the masked images contained in

the visual data will be recovered, or the entirety of the video recording will be decrypted and sent to the administrator in the form of original visual information [5–9]. The original footage contains recovered identification information regarding not only the target being tracked, but also the others whose images are captured on the same video, which may seriously compromise the privacy of those non-target individuals [10–13].

The captured images may also be used as a means to check the status of the patient in an AI-based intelligent health care system. In this case, there is a possibility that the identification information of the patient identified through the image is exposed, and the privacy of the subject may be infringed [14,15].

This paper aims to introduce a mechanism that will allow the administrators who access target(s) recorded on visual data to perform individual masking to the extent that is granted to them by the level of access right they have. The individualized masking will prevent non-accessible visual data from being leaked, and help minimize the violation of the privacy of non-target individuals and ensure their privacy [16–18]. The study comprises three chapters. Section 2 examines the previous technologies while Section 3 introduces the proposed masking mechanism that specifies identification information on surveillance footage according to the level of access permission. Section 4 compares and analyzes the existing methodology and proposes a mechanism to present differences between the two [19–22].

2. Examination of the Existing Patented Masking Technique

A wide range of studies are in progress for protecting the privacy of individuals whose images are exposed in video footage that is recorded on VSS. In South Korea, such efforts are being commercialized mostly in the form of security systems that address video image clearance. The following section examines the privacy masking systems that are commercially available in the business market.

2.1. Masking Techniques and Devices

Privacy masking techniques capture the frames that make up visual information. Then they mask one or more pieces of identification information present in each frame, insert the masked information into the frame, and store the visual information as a cluster of such frames [23]. A masking device consists of a filming module where images are recorded so that the frames can be extracted, a processing module that implements masking to each frame in the video, and a storage module for storing the frames where the masked information has been inserted. The patented technique herein under review performs masking on recorded images, and the specific key values used for the masking are utilized later on for the process of unmasking. The masked information is stored in each frame that has been masked. The target of privacy masking is the face of a person or a license plate on a vehicle (Figure 1) [24–27].

Figure 1. Flowchart showing privacy masking techniques and devices.

2.2. Face Detection-Enabled Privacy Protection Techniques and Equipment Utilized on Moving Objects

Techniques using face detection on a moving object that is being recorded on surveillance video aim to protect the privacy of the pedestrians who are also being recorded. Those techniques break the video streams into frames that include the visual information upon which masking is to be performed. Then they extract the images of a target object or objects in each frame concerned and mask them. Equipment that executes the techniques is composed of: a server that stores the video images; a frame extraction module that sequentially extracts the frames that require masking; an object extraction module that detects faces appearing in the frames that are extracted by the frame extraction module; a masking module that generates authentication keys; and a database (DB) where the generated keys are managed (Figure 2) [28–30]. The patented masking techniques replace the original video information with masked visual images, and decryption keys for the masking are stored in the DB. Regarding the scope of masking, the techniques automatically detect pedestrians in long-distance sensing and faces in short distance sensing. The moving objects so detected are subject to masking as deemed relevant. Authentication keys for the masked images are stored in the DB, and watermarks from the stored keys are extracted and used later on for recovering the images [31,32].

Figure 2. Flowchart showing face detection-enabled privacy protection techniques and equipment utilized on moving objects.

2.3. Video Manipulation Methods and Devices That Support Privacy Protection

Video manipulation methods and devices that support privacy protection aim at preventing privacy infiltration when the images recorded on multiple VSSs are required to be sent to outside entity/entities that are beyond the jurisdiction of the VSSs. In cases where the video images are requested by, for example, law enforcement agencies, masking will be carried out with a receiver of control signals activated (Figure 3) [33]. When motion signals are received, the VSS will compare the operational status of the cameras against the regulatory information and check if they match. If they don't, the system will transmit the match-failure result to the administrator. The invention comprises a storage module that stores the video images; an interface module that receives user input signals; an image processing module that performs masking on the portions of the video that are highly susceptible to privacy infiltration; and a control unit that sends out the masked images to outside entities [34,35]. The patented invention generates additional storage for masking within the storage module for the specific purposes of storing masked images and sending them to the user. The scope of masking refers to where the identification information is contained; however, the scope is designated manually [36].

Figure 3. Flowchart showing video manipulation methods and devices that support privacy protection.

3. Proposed Masking Mechanism That Limits Accessible Video Information Based on Access Permission Levels

The mechanism proposed by this study (hereinafter, the “Proposed Mechanism”) records the video images, stores them in the DB which is exclusive to that purpose, extracts object(s) with identification information that will allow the guessing of specific individual(s) whose images are found in the images, compares the extracted information against the identification information stored in the identification DB, and verifies if the individual(s) actually have the identification information concerned [37].

When the images are later requested by a user with proper access permission, the Proposed Mechanism will implement masking to the extent that matches the level of access permission he/she has, on object(s) that exceed the permission level. Regarding the other objects in the same images that are within the scope of the access permission level, the Mechanism will provide the user with the information about them in the form of original video images [38,39]. The Proposed Mechanism consists of an image collection module, an image DB module, an image services module, an object extraction module, an identification DB module, an object identification module, an access permission DB module, and a masking module. Figure 4 illustrates the sequences in which the Mechanism proceeds [40–43].

Figure 4. Flowchart showing the Proposed Mechanism that masks objects with identification information exceeding access permission.

Figure 5 shows the proposed mechanism. In the proposed mechanism, the identification object is extracted from the captured image, the object is masked and stored in the cloud server. If a request for the image is received, Only the masking of the authorized access object in the image is performed, and the restored image is provided to the user [44,45].

Figure 5. Diagram showing the Proposed Mechanism that masks objects with identification information exceeding access permission.

3.1. Image Collection Module

This module collects visual information from the recording media that transmits the visual information, which may contain videos and images. Outside entities to which the visual information is sent can include multiple CCTVs, universal serial buses (USBs), Internet protocol (IP) cameras, and other devices that are included in VSSs [46,47].

3.2. Image DB Module

This module is storage that retains the visual information received from the recording media used for the image collection module. As such, the image DB module stores the visual information for the purpose of masking, and also contains the original video information for detecting object(s) that will lead to the identification information contained in the visual information. The module does not store masked visual information that is generated upon requests from users, hence no additional storage is required [48–50].

3.3. Image Services Module

When a user with legitimate access permission submits a request for releasing certain visual information, the image services module will receive from the masking module the identification information masked by the masking module on the identification information that is contained in the visual information and that exceeds the requesting user's access permission. The masking is carried out to the extent that matches the level of access permission the user has. Then the image services module transmits the masked information to the user as a response to the request. The module may adjust the number of visual data that are provided to the extent that matches the user's access permission, as well as the accessible VSSs [51–53].

3.4. Object Extraction Module

This module extracts personal identification information that will allow the guessing of particular individual(s) who are predefined as such. The identification information may contain the face of the individual(s) or a license plate on a vehicle. The object extraction module searches for the features related to the identification information regarding the object(s) that appear in the static images, and then extracts all objects within the portions of the video which presumably have the identification information on that individual(s). Available feature extraction techniques include knowledge-based extraction

methods, feature-based approaches, template-based matching techniques, and appearance-based algorithms. Using these, one extracts the personal identification information contained in the video information [54,55].

3.5. Object Identification Module

This module compares the data that were extracted by the object extraction module on particular object(s) using the identification information that presumably recognizes the object(s), against the data that are stored in the identification DB module where all identification information is retained. The comparison allows the object identification module to calculate the similarities between the parameters for the identification markers in the visual information extracted by the object extraction module, and the identification information stored in the identification DB module. Based on the comparison results, the object identification module recognizes object(s) showing similarities at or above a certain level. The object identification module executes recognition only on the information extracted by the object extraction module and as such, it uses system resources that are less than those that would be necessary if the entirety of the visual information was subject to recognition [56].

3.6. Identification DB Module

The identification DB module is storage retaining the identification data that will allow the recognition of visual information where the guessing of particular individual(s) can be made in comparison with the object(s) concerned. The identification data to be stored in this module refer to the information that leads to the recognition of particular object(s) based on a comparison against the features extracted by the object extraction module. The identification data offer information that is used to recognize object(s), including a specific individual who is recognizable as a person registered in the system as a criminal, a marker that aims at distinguishing males from females, and information regarding a license plate on a certain vehicle [57–59].

3.7. Masking Module

The masking module has the authorization for checking/verifying the access permission granted to the user to ensure that he/she has the proper clearance for accessing the access permission DB module. The masking module also checks the access permission possessed by the user, through the access permission DB module on each object that has been extracted, and can perform individual masking on objects to the extent that is allowed by the access rights granted to the user [60]. Additionally, the masking module provides masking on object(s) that exceed the access rights of the user as stated in the access permission DB module when a request for accessing visual information is approved via the image services module, and then returns the masked images to the image services module. Masking techniques obfuscate the images by manipulating or utilizing colors, shades, brightness, chroma, silhouette, image mosaic, blending, and blurring. When masking any object that has been extracted, the masking module verifies the status of the access permission granted to the user and proceeds with the masking only on those not covered by the user's access right. Unlike the existing methods, the masking offered by the Proposed Mechanism obfuscates identification information contained in the visual information in phases, i.e., according to the levels of access permission [61].

3.8. Access Permission DB Module

The access permission DB module is storage that grants access to authenticated users and has rules for masking the video images to be sent, according to the level of access permission. As the masking module performs masking on objects that have been recognized by the object identification module, the access permission DB module holds authentication information that discerns the status of the access permission granted to the user on each object (allowed vs. denied) and offers authentication information regarding each object upon requests from the masking module. Depending on the level of access rights stored in the access permission DB module, requesters of visual information may

obtain different results from the same visual information due to the difference in the scope of masking provided [62–65].

4. Comparison and Analysis of the Proposed and Existing Mechanisms

This chapter analyzes the Proposed Mechanism and the existing mechanisms presented herein. Based on the analysis, differences between the two are addressed. Specifically, four features are examined to be unique to the Proposed Mechanism, namely masking performed on identification information contained in the visual information, provision of images as requested by the user, division of visual information storage within the image DB, and selection of targets for masking based on the level of access permission.

4.1. Comparisons Amongst Privacy Masking Techniques and Devices

Figure 6 illustrates a mechanism embodied in privacy masking techniques and devices which automatically extracts identification information present in the visual information and masks and stores the image information only as masked data. Additionally, this mechanism stores the original video recording as masked images, hence it requires separate storage for retaining the additional data. The mechanism masks all identification information regardless of the level of access permission.

Figure 6. Comparisons amongst privacy masking techniques and devices.

4.2. A Face Recognition-Based Privacy Protection Technique and Equipment Used on Moving Pedestrians—Comparison and Analysis

Figure 7 shows the corresponding portion of a face-recognition-based privacy protection technique and equipment that are used on moving pedestrians. Unless otherwise requested by a user, this mechanism automatically masks the visual images being recorded and then stores the unmasking keys in a separate DB and only the masked visual information in the regular DB. When receiving a user's request for visual information, the mechanism decrypts the masked images by using the stored unmasking keys and offers the information to the user. In that process, the unmasking will apply to all

of the identification information contained in the visual data requested. Hence, the mechanism ends up offering more than the minimum identification information the user has requested.

Figure 7. Corresponding features of a face-recognition-based privacy protection technique and equipment used on moving pedestrians.

4.3. A Visual Information Processing Method and Equipment That Supports Privacy Protection—Comparison and Analysis

Figure 8 lists the corresponding feature of another mechanism in comparison with the proposed mechanism involving visual information processing methods and devices that support the protection of privacy. This mechanism masks the identification information within the visual data before transmitting it when the data including the identification information are requested to be sent out. The masked images are stored separately from the unmasked original visual information, and this requires additional storage. The coverage by masking will be achieved regardless of the level of access permission held by the requester of the visual information.

Figure 8. Corresponding feature of a visual information processing method and equipment that support privacy protection.

4.4. Distinctive Features of the Proposed Mechanism

The Proposed Mechanism distinguishes itself from the above-mentioned approaches that adopt a mechanism of masking the identification information contained in the visual data or other conventional mechanisms. The distinction lies in the features of the Proposed Mechanism where a separate module is deployed to store the access permission granted to the potential requesters of visual information, ensuring that the visual information is not released to any other requesters outside the limits of access permission. Moreover, the Mechanism masks any identifying information that is not authorized, so that only the permitted identification information is released to the authorized requesters only. Figure 9 summarizes the process of the Proposed Mechanism performing masking on visual information.

Figure 9. Distinctive features of the Proposed Mechanism.

The masking processing mechanism of the general video surveillance system extracts all the identification objects existing in the photographed image as shown in Figure 10a, and performs masking collectively. At this time, if the masking image processed in batch is restored, unmasking is performed on all masked objects existing in the image. Reconstructed images for all non-identified objects can cause unnecessary privacy breach controversy. However, the masking restoration mechanism proposed in this paper minimizes unnecessary privacy infringement by allocating the access rights of the masking object existing in the image and maintaining the masking of the identification object which is out of the access rights of the requesting user.

(a) Masking process of general video surveillance system.

(b) The process of the proposed video surveillance system masking mechanism

Figure 10. General masking and restoration process and masking and restoration process of proposed mechanism.

Table 1 lists the differences between the existing techniques and the Proposed Mechanism.

Table 1. Comparison and analysis of the Proposed Mechanism and the existing methods.

Comparison Item	Patent 1	Patent 2	Patent 3	The Proposed Mechanism
Apply to mask	O	O	O	O
Processing by user request	X	O	O	O
Store only the original image in the repository	X	X	O	O
Partial masking according to the access authority	X	X	X	O

5. Conclusion and Future Plans

Visual images recorded on a visual surveillance system (VSS) are used by the administrators who control the system. In that process, personal identification information contained in the video images can be leaked, offering identification information that exceeds what is needed to be communicated by the administrators. Typically, privacy masking is implemented on the entirety of video images, and the process of unmasking renders all of the identification information within the visual images decrypted non-differentially. Such practices imply that the identification information regarding third parties and not just the target(s) being recorded can be released to users.

The main section of this study investigated the existing techniques applied to VSS and examined the differences between those techniques and the mechanism herein proposed (the “Proposed Mechanism”).

The Proposed Mechanism masks video images recorded on a VSS as it transmits them to a user upon request. Depending on the level of access rights granted to the requesting user, the Mechanism views all identification information contained in the video as respective objects and as such, it masks any identification information exceeding the access permission enjoyed by the user upon the comparison. Such a process prevents the leakage of identification information regarding individuals/objects other than the one(s) targeted. The main feature of the Proposed Mechanism is the implementation of masking to the extent that matches the level of access permission.

This method aims to secure the privacy of the object by protecting the identification information by stepwise restoring the masking area of the photographed subject in accordance with the authority of the access requester. This method confirms the state of the patient based on the image. It can also be applied to healthcare systems.

Non-differential unmasking approaches, now commonly adopted, can increase the channels of identification information leakage, and this concern over privacy infiltration is being voiced increasingly more vehemently given the increasing number of VSSs each year. To address the issue, only the minimum of identification information within the video images requested should be released to users. This solution is embodied in the Proposed Mechanism of masking which differentially masks personal identification information to the level of access permission, thus minimizing the released identification information as well as the channels of leakage.

Currently, the downside of VSS is being implicitly overlooked for the purpose of ensuring public safety. Nonetheless, solutions should be studied taking advantage of the advancement in big data analytics technology so that the identification information included in visual images can be contained to minimize the channels of leaking personal information of the objects recorded on VSS. We plan to implement more sophisticated mechanisms by updating the proposed algorithms in the future.

Author Contributions: Conceptualization, N.P.; Data curation, J.K.; Methodology, B.-G.K.; Project administration, N.P.; Writing—original draft, N.P.

Funding: This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) [2019-0-00203, The Development of Predictive Visual Security Technology for Preemptive Threat Response]. And, this research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2019R111A3A01062789).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yuxi, P.; Luuk, J.S.; Raymond, N.J.V. Low-resolution face recognition and the importance of proper alignment. *IET Biom.* **2019**, *8*, 267–276.
2. Ling, J.; Zhang, K.; Zhang, Y.; Yang, D.; Chen, Z. A saliency prediction model on 360 degree images using color dictionary based sparse representation. *Signal Process. Image Commun.* **2018**, *69*, 60–68. [[CrossRef](#)]
3. Germain, S.; Douillet, A.C.; Dumoulin, L. The Legitimization of Cctv as a Policy Tool: Genesis and Stabilization of a Socio-Technical Device in Three French Cities. *Br. J. Criminol.* **2012**, *52*, 294–308. [[CrossRef](#)]
4. Kim, J.; Park, N.; Kim, G.; Jin, S. CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia. *Electronics* **2019**, *8*, 412. [[CrossRef](#)]
5. Madine, F.; Akhaee, M.; Zarmehi, N. A multiplicative video watermarking robust to H.264/AVC compression standard. *Signal Process. Image Commun.* **2018**, *68*, 229–240. [[CrossRef](#)]
6. SanMiguel, J.C.; Martínez, J.M. Use of feedback strategies in the detection of events for videosurveillance. *IET Comput. Vis.* **2012**, *5*, 309–319. [[CrossRef](#)]
7. SanMiguel, J.C.; Martínez, J.M. Pixel-based colour contrast for abandoned and stolen object discrimination in video surveillance. *Electron. Lett.* **2012**, *48*, 86–87. [[CrossRef](#)]
8. Short, E.; Ditton, J. Seen and Now Heard: Talking to the Targets of Open Street CCTV. *Br. J. Criminol.* **1998**, *38*, 404–428. [[CrossRef](#)]
9. Park, N.; Kim, M. Implementation of load management application system using smart grid privacy policy in energy management service environment. *Clust. Comput.* **2014**, *17*, 653–664. [[CrossRef](#)]
10. Tianjun, M.; Qingge, J.; Ning, L. Scene invariant crowd counting using multi-scales head detection in video surveillance. *IET Image Process.* **2018**, *12*, 2258–2263.
11. Fan, M.; Wang, H. An enhanced fragile watermarking scheme to digital image protection and self-recovery. *Signal Process. Image Commun.* **2018**, *67*, 19–29. [[CrossRef](#)]
12. Guan, J.; Wang, E. Repeated review based image captioning for image evidence review. *Signal Process. Image Commun.* **2018**, *63*, 141–148. [[CrossRef](#)]
13. Goold, B.; Loader, I.; Thumala, A. The Banality of Security: The Curious Case of Surveillance Cameras. *Br. J. Criminol.* **2013**, *53*, 977–996. [[CrossRef](#)]
14. Hu, Y.; Lu, X. Learning spatial-temporal features for video copy detection by the combination of CNN and RNN. *J. Vis. Commun. Image Represent.* **2018**, *55*, 21–29. [[CrossRef](#)]
15. Tzelepi, M.; Tefas, A. Deep convolutional image retrieval: A general framework. *Signal Process. Image Commun.* **2018**, *63*, 30–43. [[CrossRef](#)]
16. McCahill, M. CCTV and Policing: Public Area Surveillance and Police Practices in Britain. *Br. J. Criminol.* **2005**, *45*, 234–236. [[CrossRef](#)]
17. Wu, H.; Li, Y.; Bi, X.; Zhang, L.; Bie, R.; Wang, Y. Joint entropy based learning model for image retrieval. *J. Vis. Commun. Image Represent.* **2018**, *55*, 415–423. [[CrossRef](#)]
18. Leung, V.; Colombo, A.; Orwell, J.; Velastin, S.A. Modelling periodic scene elements for visual surveillance. *IET Comput. Vis.* **2001**, *37*, 20–21. [[CrossRef](#)]
19. Loideain, N.N. Cape Town as a smart and safe city: Implications for governance and data privacy. *Int. Data Priv. Law* **2017**, *7*, 314–334. [[CrossRef](#)]
20. Lee, D.; Park, N. Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance. *Supercomputing* **2017**, *73*, 1119. [[CrossRef](#)]
21. Ayesha, C.; Santanu, C. Video analytics revisited. *IET Comput. Vis.* **2016**, *10*, 237–249.
22. Pons, J.; Prades-Nebot, J.; Albiol, A.; Molina, J. Fast motion detection in compressed domain for video surveillance. *Electron. Lett.* **2002**, *38*, 409–411. [[CrossRef](#)]
23. Du, H.; Hu, Q.; Jiang, M.; Zhang, F. Two-dimensional principal component analysis based on Schattenp-norm for image feature extraction. *J. Vis. Commun. Image Represent.* **2015**, *32*, 55–62. [[CrossRef](#)]
24. Pinto, T. Who controls the Naomi Campbell information flow? A practical analysis of the law of privacy. *J. Intellect. Prop. Law Pract.* **2006**, *1*, 354–361. [[CrossRef](#)]
25. Hsia, S.C.; Wang, S.H. Adaptive video coding control for real-time H.264/AVC encoder. *J. Vis. Commun. Image Represent.* **2009**, *20*, 463–477. [[CrossRef](#)]

26. Haiyun Guo; Jinqiao Wang; Hanqing Lu. Multiple deep features learning for object retrieval in surveillance videos. *IET Comput. Vis.* **2016**, *10*, 268–272. [[CrossRef](#)]
27. Greek, C.E. Criminal Visions: Media Representations of Crime and Justice. By Paul Mason. *Br. J. Criminol.* **2005**, *45*, 230–232. [[CrossRef](#)]
28. Huang, P.; Tang, Z.; Chen, C.; Yang, Z. Local maximal margin discriminant embedding for face recognition. *J. Vis. Commun. Image Represent.* **2014**, *25*, 296–305. [[CrossRef](#)]
29. Bhagat, P.K.; Choudhary, P. Image annotation: Then and now. *Image Vis. Comput.* **2018**, *80*, 1–23. [[CrossRef](#)]
30. Cucchiara, R.; Grana, C.; Prati, A.; Vezzani, R. Computer vision system for in-house video surveillance. *IEEE Proc. Vis. Image Signal Process.* **2005**, *152*, 242–249. [[CrossRef](#)]
31. Lee, D.; Park, N.; Kim, G.; Jin, S. De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment. *Peer Peer Netw. Appl.* **2018**, *11*, 1299–1308. [[CrossRef](#)]
32. Azhar, H.; Amer, A. Classification of surveillance video objects using chaotic series. *IET Image Process.* **2012**, *6*, 919–931. [[CrossRef](#)]
33. Zhang, L.; Dou, P.; Kakadiaris, I.A. Patch-based face recognition using a hierarchical multi-label matcher. *Image Vis. Comput.* **2018**, *73*, 28–39. [[CrossRef](#)]
34. Hu, J. Discriminative transfer learning with sparsity regularization for single-sample face recognition. *Image Vis. Comput.* **2017**, *60*, 48–57. [[CrossRef](#)]
35. Li, H.; Achim, A.; Bull, D. Unsupervised video anomaly detection using feature clustering. *IET Signal Process.* **2012**, *6*, 521–533. [[CrossRef](#)]
36. Balasubramanian, Y.; Sivasankaran, K.; Krishraj, S.P. Forensic video solution using facial feature-based synoptic VideoFootage Record. *IET Comput. Vis.* **2016**, *10*, 315–322. [[CrossRef](#)]
37. Yi, H.; Nong, S.; Changxin, G.; Jun, H. Online Unsupervised Learning Classification of Pedestrian and Vehicle for Video Surveillance. *Chin. J. Electron.* **2017**, *26*, 145–151.
38. Liu, J.; Liu, B.; Zhang, S.; Yang, F.; Yang, P.; Metaxas, D.N.; Neidle, C. Non-manual grammatical marker recognition based on multi-scale. spatio-temporal analysis of head pose and facial expressions. *Image Vis. Comput.* **2014**, *32*, 671–681. [[CrossRef](#)]
39. Watson, S. Faster Higher Stronger Secure. *ITNOW* **2012**, *54*, 12–15. [[CrossRef](#)]
40. Hagmann, J. Security in the Society of Control: The Politics and Practices of Securing Urban Spaces. *Int. Polit. Sociol.* **2017**, *11*, 418–438. [[CrossRef](#)]
41. Park, N.; Lee, D. Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment. *Pers. Ubiquitous Comput.* **2018**, *22*, 3–10. [[CrossRef](#)]
42. Yan, J.; Zhang, X.; Lei, Z.; Li, S.Z. Face detection by structural models. *Image Vis. Comput.* **2014**, *32*, 790–799. [[CrossRef](#)]
43. Chen, W.-G.; Ling, Y. Noise variance adaptive successive elimination algorithm for block motion estimation: Application for video surveillance. *IET Signal Process.* **2007**, *1*, 150–155. [[CrossRef](#)]
44. Park, N.; Kang, N. Mutual authentication scheme in secure internet of things technology for comfortable lifestyle. *Sensors* **2016**, *16*, 20. [[CrossRef](#)] [[PubMed](#)]
45. Ziani, A.; Motamed, C.; Noyer, J.-C. Temporal reasoning for scenario recognition in video-surveillance using Bayesian networks. *IET Comput. Vis.* **2008**, *2*, 99–107. [[CrossRef](#)]
46. Lee, K.; Yeuk, H.; Kim, J.; Park, H.; Yim, K. An efficient key management solution for privacy masking, restoring and user authentication for video surveillance servers. *Comput. Stand. Interfaces* **2016**, *44*, 137–143. [[CrossRef](#)]
47. Vijayakumar, P.; Chang, V.; Deborah, L.J.; Balusamy, B.; Shynu, P.G. Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks. *Future Gener. Comput. Syst.* **2018**, *78*, 943–955. [[CrossRef](#)]
48. Diaz, J.; Arroyo, D.; Rodriguez, F.B. A formal methodology for integral security design and verification of network protocols. *J. Syst. Softw.* **2014**, *89*, 87–98. [[CrossRef](#)]
49. Lee, K.; Yim, K.; Mikki, M.A. A secure framework of the surveillance video network integrating heterogeneous video formats and protocols. *Comput. Math. Appl.* **2012**, *63*, 525–535. [[CrossRef](#)]
50. Gope, P. LAAP: Lightweight Anonymous Authentication Protocol for D2D-Aided Fog Computing Paradigm. *Comput. Secur.* **2019**, *86*, 223–237. [[CrossRef](#)]

51. Choi, L.K.; Bovik, A.C. Video quality assessment accounting for temporal visual masking of local flicker. *Signal Process. Image Commun.* **2018**, *67*, 182–198. [[CrossRef](#)]
52. Koscinski, I.; El Alaoui-Lasmali, K.; Di Patrizio, P.; Kohler, C. Videos for embryology teaching. power and weakness of an innovative tool. *Morphologie* **2019**, *103*, 72–79. [[CrossRef](#)] [[PubMed](#)]
53. Wen, H.; Zhou, X.; Sun, Y.; Zhang, J.; Yan, C. Deep fusion based video saliency detection. *J. Vis. Commun. Image Represent.* **2019**, *62*, 279–285. [[CrossRef](#)]
54. Ding, G.; Khan, S.; Tang, Z.; Porikli, F. Feature mask network for person re-identification. *Pattern Recognit. Lett.* **2019**, in press. [[CrossRef](#)]
55. Zhan, Z.; Yang, X.; Li, Y.; Pang, C. Video deblurring via motion compensation and adaptive information fusion. *Neurocomputing* **2019**, *341*, 88–98. [[CrossRef](#)]
56. Du, L.; Zhang, W.; Fu, H.; Ren, W.; Zhang, X. An efficient privacy protection scheme for data security in video surveillance. *J. Vis. Commun. Image Represent.* **2019**, *59*, 347–362. [[CrossRef](#)]
57. Tsakanikas, V.; Dagiuklas, T. Video surveillance systems-current status and future trends. *Comput. Electr. Eng.* **2018**, *70*, 736–753. [[CrossRef](#)]
58. Guttman, M.; Wolf, L.; Cohen-Or, D. Content aware video manipulation. *Comput. Vis. Image Underst.* **2011**, *115*, 1662–1678. [[CrossRef](#)]
59. Niu, G.; Chen, Q. Learning an video frame-based face detection system for security fields. *J. Vis. Commun. Image Represent.* **2018**, *55*, 457–463. [[CrossRef](#)]
60. Chhokra, P.; Chowdhury, A.; Goswami, G.; Vatsa, M.; Singh, R. Unconstrained Kinect video face database. *Inf. Fusion* **2018**, *44*, 113–125. [[CrossRef](#)]
61. Arceda, V.E.M.; Fabián, K.M.F.; Laura, P.C.L.; Tito, J.J.R.; Cáceres, J.C.G. Fingertip Detection and Tracking for Recognition of Air-Writing in Videos. *Expert Syst. Appl.* **2019**, in press.
62. Mutneja, V.; Singh, S. GPU accelerated face detection from low resolution surveillance videos using motion and skin color segmentation. *Optik* **2018**, *157*, 1155–1165. [[CrossRef](#)]
63. Rashedi, E.; Barati, E.; Nokleby, M.; Chen, X. “Stream loss”: ConvNet learning for face verification using unlabeled videos in the wild. *Neurocomputing* **2019**, *329*, 311–319. [[CrossRef](#)]
64. Wang, L.; Yu, X.; Bourlai, T.; Metaxas, D.N. A coupled encoder–decoder network for joint face detection and landmark localization. *Image Vis. Comput.* **2019**, *87*, 37–46. [[CrossRef](#)]
65. Creasey, M.S.; Albalooshi, F.A.; Rajarajan, M. Continuous face authentication scheme for mobile devices with tracking and liveness detection. *Microprocess. Microsyst.* **2018**, *63*, 147–157. [[CrossRef](#)]

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).